Listing and Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (CURRENTLY AMENDED) A method for managing access to an electronic device, said method comprising:

(a) sending a first message from a first electronic device to a second electronic device;

(b) receiving, in said first electronic device, from said second electronic device a digital certificate encrypted using a first private key of said second electronic device;

(c) receiving, in said first electronic device, from said second electronic device said first message encrypted using a second private key of said second electronic device;

(d) authenticating said second electronic device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second electronic devices in response to the authentication of said second electronic device.

2. (Currently Amended) The method of Claim 1 wherein said first message comprises first identification data associated with said first electronic device and a date and time stamp.

3. (Currently Amended) The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second electronic device and a second public key of said second electronic device.

4. (Currently Amended) The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first electronic device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

(c) comparing said first decrypted message to said first message.

5. (Currently Amended) The method of Claim 4 wherein said first public key is stored in said first electronic device.

6. (Cancelled)

7. (Currently Amended) The method of Claim [[6]] 22 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second electronic device.

8. (Currently Amended) The method of Claim 7 wherein said first electronic device is a set-top box and said second electronic device is a server associated with a service provider, the set-top box having a smart card with service provider identification data stored therein coupled thereto, the set-top box sending said first message to said server in response to authentication of said smart card and said service provider identification data.

9. (Original) The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. (Currently Amended) A method for managing access to an electronic device, said method comprising:

(a) sending first identification data associated with a first electronic device to a second electronic device;

(b) receiving, in said first electronic device, from said second electronic device a digital certificate encrypted using a first private key of said second electronic device, said digital certificate having second identification data associated with said second electronic device and a second public key of said second electronic device;

(c) encrypting said first identification data in said second electronic device using a second private key associated with said second electronic device to generate first encrypted identification data;

(d) receiving, in said first electronic device, from said second electronic device said first encrypted identification data;

(e) decrypting in said first electronic device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first electronic device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second electronic device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second electronic device second encrypted identification data, said second encrypted identification data being encrypted in said first electronic device using said second public key of said second electronic device; and

(i) establishing a communication channel between said first and said second electronic devices.

11. (Previously Presented) A method for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. (Previously Presented) The method of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. (Previously Presented) The method of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. (Previously Presented) The method of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. (Previously Presented) The method of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. (Previously Presented) The method of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. (Previously Presented) The method of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. (Previously Presented) The method of Claim 17 wherein said first digital certificate is stored in said smart card.

19. (Previously Presented) The method of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

20. (Previously Presented) The method of Claim 19 wherein said second digital certificate is stored in said service provider.

21. (New) A method for managing access between a plurality of electronic devices, comprising:

sending first message data from a first electronic device to a second electronic device;

receiving, in said first electronic device, from said second electronic device, second data being indicative of a digital certificate encrypted using a first private key of said second electronic device;

receiving, in said first electronic device, from said second electronic device, said first message data being encrypted using a second private key of said second electronic device;

authenticating said second electronic device in response to said digital certificate and said first encrypted message;

establishing a communication channel between said first and said second electronic devices in response to the authentication of said second electronic device;

encrypting said first message using a public key to generate a second encrypted message; and

sending data indicative of said second encrypted message to said second electronic device.

22. (New) A method for managing access between a plurality of electronic devices, comprising:

sending first message data from a first electronic device to a second electronic device, the first message data comprising first identification data associated with said first electronic device and a date and time stamp;

receiving, in said first electronic device, from said second device digital certificate data encrypted using a first private key of said second electronic device, said digital certificate data comprising second identification data associated with said second electronic device and a second public key of said second electronic device;

receiving, in said first electronic device, from said second electronic device said first message data encrypted using a second private key of said second electronic device;

authenticating said second electronic device in response to said digital certificate data and said encrypted first message data;

establishing a communication channel between said first and said second electronic devices in response to the authentication of said second electronic device;

encrypting said first message data using a public key to generate a second encrypted message data; and,

sending said second encrypted message data to said second electronic device;

wherein, said authenticating comprises: decrypting said digital certificate in said first device using a first public key stored in said first electronic device; decrypting said first encrypted message using said public key used to generate said second encrypted message to generate a first decrypted message; and comparing said first decrypted message to said first message.